performing a boot procedure that includes the secure processor deriving the first cryptographic key based on a first entropy value stored in the secure memory.

45. A method, comprising:

maintaining, by a computing device, a file system that includes encrypted data and a plurality of encrypted entropy values usable to derive cryptographic keys encrypting the data;

sending, by a main processor of the computing device, an access request to a secure processor of the computing device;

in response to the access request:

using, by the secure processor, a first cryptographic key stored in secure memory to decrypt one of the plurality of entropy values, wherein the secure memory is inaccessible to the main processor; and

applying, by the secure processor, a key derivation function to the decrypted entropy value to derive a second cryptographic key that encrypts data stored in the file system.

46. The method of claim **45**, further comprising:

receiving, by the secure processor, a revocation request to revoke access to the second cryptographic key; and

in response to the revocation request, the secure processor removing the first cryptographic key from the secure memory to prevent a subsequent decryption of the encrypted entropy value and a subsequent derivation of the second cryptographic key.

47. The method of claim **45**, further comprising:

performing, by the computing device, a boot process that includes the secure processor deriving the first cryptographic key based on an entropy value stored in the secure memory, wherein the first cryptographic key protects data of an operating system booted in the boot process.

48. The method of claim **45**, further comprising:

receiving, by the secure processor, a replacement request to replace the second cryptographic key with a third cryptographic key; and

in response to the replacement request, the secure processor storing the entropy value of the second cryptographic key in the secure memory until the secure processor receives a confirmation that an entropy value of the third cryptographic key has successfully been stored in the file system.

* * * * *